INTELLIGENCE COMMUNITY STANDARD

502-02

Host-Based Security

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, United States Intelligence Activities, as amended; Intelligence Community Directive (ICD) ICD 500, *Director of National Intelligence Chief Information Officer*; ICD 502, *Integrated Defense of the Intelligence Community Information Environment*; and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Standard (ICS) establishes standards for the Intelligence Community (IC) information environment (IE) host-based security capabilities and reporting security information on IC element hosts to the IC Incident Response Center (IC-IRC). When fully implemented, the IC IE host-based security framework will enhance the protection of IC hosts, including hosts in the IC Information Technology Enterprise (ITE), and increase shared situational awareness.

C. APPLICABILITY

1. This Standard applies to the IC, as defined by the National Security Act of 1947, as amended, and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

2. This Standard applies to all hosts in the IC IE (workstations and servers), owned or operated by the IC element, independent of classification (Unclassified, Secret, Top Secret) with the ability to run a host-based agent unless waivered in accordance with this Standard. This Standard also applies to workstations and servers running in a virtual environment and those running as part of IC ITE resources.

3. This Standard applies to the *Host-Based Security Information Sharing* Enterprise Standard.[1]

D. IMPLEMENTATION

1. IC elements must integrate host-based security with their ICD 503 Risk Management Framework (RMF) continuous monitoring program.

2. IC elements may, consistent with DNI direction, implement more stringent requirements than those of this Standard as necessary to support their respective missions and internal security requirements to the extent that it will not inhibit situational awareness and authorized information sharing.

[1] In accordance with ICS 500-20, *Intelligence Community Enterprise Standards Compliance*, IC elements shall consult the IC Enterprise Standards Baseline (ESB) for compliance requirements associated with each version of a document included therein. Each version will be individually registered in the IC ESB. The IC ESB will define, among other things, the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

3. If an IC element cannot support a requirement of this Standard, a waiver may be granted for implementing the requirement.

a. For IC ITE services of common concern and systems in the shared environment, all waivers from the requirements in this Standard shall be submitted to the IC CIO for review and approval. To ensure timely consideration, waiver requests shall identify the specific implementation requirements at issue and, as appropriate, state the cost, schedule, operational performance, and information security impacts that would be incurred without the waiver. Waiver requests, as appropriate, shall also describe a transition plan for eventual compliance with the specific requirements at issue. The IC CIO will respond to all waiver requests within 30 business days of the date of submittal.

b. For informational purposes, all non-ITE systems systems in the IC IE which do not meet the requirements of this ICS, shall report discrepancies to the IC CIO and, as appropriate, state the cost, schedule, operational performance, and information security impacts that would be incurred in order to achieve full compliance.

4. Participating organizations may elect to implement some of the capabilities of this Standard through subscriber-based service agreements with other IC elements. When subscribing services from another organization, the subscriber must ensure that the provider has agreed in a formal Service Level Agreement (SLA) to implement the requirements in this Standard.

E. RESPONSIBILITIES

1. IC elements shall:

a. When designated as providing services of common concern, implement this Standard on behalf of subscribed, serviced, and supported IC elements and organizations.

b. Implement the host-based security capabilities outlined in this Standard to detect, prevent, and report anomalous (outside user norms) or noncompliant activity (in violation of established rule sets) occurring on their host machines that will enable effective and timely response generation in accordance with established IC-IRC reporting timelines as outlined in reference 5.

c. Establish collaboration and information sharing processes for implementing host-based security capabilities that include, as applicable, the following IC element organizations: personnel security, counterintelligence, law enforcement, management, information security, information technology (IT) support, legal, privacy, inspector general, public affairs, facilities management, OPSEC, and intelligence oversight.

d. Plan, fund, acquire, implement, program, and manage current and future host- based security capabilities in accordance with the guidance provided in this Standard. Include host-based security requirements in annual budget planning cycles and ensure appropriate funding for system installation, upgrade, and long-term system maintenance.

e. Establish and implement a host-based security training program to include procedures that identify, define, and designate necessary training for personnel conducting host-based security activities.

f. Ensure that host-based asset and configuration management information is aggregated and made available to the element's computer network defense (CND) operational focal point and leadership.

g. Ensure that host-based anomalies and security incidents are reported through the organization's CND operational focal point to the IC-IRC in accordance with *IC Incident Reporting Procedures*.

h. Conduct trend analysis, review audit logs, and reassess existing configuration and protection requirements in response to anomalies and incidents.

i. Implement and maintain change management processes (e.g., signature updates, sensor tuning) when available and that adhere to the IC element and IC-IRC's host-based protection requirements.

j. Provide reports to the IC-IRC through the identified IC element sub-organization (e.g., CERT) on a periodic and ad-hoc basis as determined by the IC CIO or designee to support IC IE situational awareness.

k. Establish and maintain a management repository that includes the following capabilities:

(1) Aggregate event and host data from multiple hosts;

(2) Store events/alerts (store event/alert data in accordance with IC element internal policies);

(3) Coordinate the communication of events, the enforcement of policies, and the updating of intrusion prevention/antivirus signatures on hosts;

(4) Transmit host information and status outlined in *Host-Based Security Information Sharing* Enterprise Standard via automated means to the IC-IRC on a daily basis;

(5) Use encrypted communications between servers using a Federal Information Processing Standard (FIPS) 140-2 certified cryptographic module;

(6) Use asset tracking with configuration baseline and configuration drift;

(7) Provide dashboards at the analytical, CND operational, and executive levels with attribute-based access controls;

(8) Import computer security related information made available from multiple vendors of host security products;

(9) Provide capability to support custom content and additional product integration.

l. Establish and maintain a host-based security capability that includes the following:

(1) Agents on each host that are configured to not interfere with the operation and collection of agents used for the detection of insider threats where utilized;

(2) Transmit events/alerts to a management server and encrypt all communications using FIPS 140-2 certified cryptographic module;

(3) Provide anti-virus/malware/spyware protection on all hosts, workstations, and servers including virtual machines;

(4) Provide Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) for all hosts, workstations, and servers including virtual machines;

(5) Configure a Firewall on workstations including virtual machines;

(6) Monitor, block, restrict, and report-on the use of removable devices and media;

(7) Monitor, block, restrict, and report on the use of embedded devices or other user peripherals and monitor device status (whether enabled or disabled);

(8) Monitor host processes via configurable Host Integrity Check that verifies the capability to compare running processes against a standard baseline for workstations, during both off network and on network operations;

(9) Provide quarantine rule set and automated remediation procedures based on host integrity check results on all hosts during both off network and on network operations;

(10) Monitor file systems via configurable host integrity tests for anomalous file system status;

(11) Monitor host configuration via a configurable Host Integrity Check for configuration drift based on compliance policy; during both off network and on network operations;

(12) Enforce security and compliance policies off-line, including connection awareness to sense and react to online/offline/online status changes.

2. The IC-IRC shall:

   a. Provide host-based situational awareness to the IC CIO or designee.

   b. Provide host-based security situational awareness reporting to IC elements.

F. EFFECTIVE DATE: This Standard becomes effective on the date of signature.

Al Tarasiuk
Assistant Director of National Intelligence and
Intelligence Community Chief Information Officer

23 Dec 2013
Date

Appendix A - References

1. Chairman of the Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Computer Network Defense (CND)*, (9 February 2011).

2. Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, (March 2011).

3. CNSS Instruction No. 4009, *A Common Information Assurance Glossary for National Security Systems*, (April 2010).

4. Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules, (May 25, 2001)*.

5. IC CIO Memorandum 2011-0463, *Intelligence Community (IC) Procedures for Reporting Incidents to the Intelligence Community Incident Response Center (IC-IRC)*, (October 25, 2011).

6. Intelligence Community Directive 500, *Director of National Intelligence Chief Information Officer*, (August 7, 2008).

7. Intelligence Community Directive 502, *Integrated Defense of the Intelligence Community Information Environment*, (March 11, 2011).

8. Intelligence Community Directive 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, (September 15, 2008).

9. SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, (February 2007).

10. Intelligence Community Standard 500-27, *Collection and Sharing of Audit Data*, (June 2, 2011).

Appendix B – Terms and Definitions

Agent: A program that performs some information gathering or processing task in the background. Typically, an agent is given a very small and well-defined task.

Computer Network Defense (CND): Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

Configuration Baseline: A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed to at a given point in time, and which can be changed only through change control procedures. The configuration baseline is used as a basis for future builds, releases, and/or changes.

Configuration Drift: Changes made over time that cause a computer or service to deviate from a desired configuration.

Continuous Monitoring: The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the IC depends. The process includes: 1) The development of a strategy to regularly evaluate selected information assurance (IA) controls, 2) Recording and evaluating information assurance relevant events and effectiveness of the IC in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information-sharing decisions involving the IC.

Embedded devices: Hardware components of a computer system that are incorporated in the overall system. Embedded devices include: network card, web-based camera, and microphone.

Event: Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

Firewall: A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

Host: A computer (desktop and portable) including servers.

Host-based Intrusion Prevention System (HIPS) – A program that monitors the characteristics of a single host and the events occurring within the host to identify and stop suspicious activity.[2]

Host-based security: Host-based security is a set of capabilities that provide a framework to implement a wide-range of security solutions on hosts. This framework includes a trusted agent and a centralized management function that together provide automated protection to detect, respond to, and report host-based vulnerabilities and incidents.

Host Integrity Check: A security mechanism that verifies the compliance of hosts to organizational policies (such as patch and anti-virus management) prior to authorizing network access.

IC Information Technology Enterprise (ITE): The strategic implementation of the IC information environment to enable greater IC integration, information sharing and safeguarding through a new common IC information technology architecture that substantially reduces costs.

---

[2] NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems. Feb 2007.

Intelligence Community Information Environment: The individuals, organizations, and information technology capabilities that collect, process, or share Sensitive Compartmented Information, or that regardless of classification, are operated by the IC and are wholly or majority National Intelligence Program-funded. The IC information environment is an interconnected shared risk environment where the risk accepted by one IC element is effectively accepted by all (IC Directive 502, *Integrated Defense of the Intelligence Community Information Environment*, {March 11, 2011}).

Intrusion Detection System (IDS): Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations).[3]

Intrusion Prevention System (IPS): System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.[4]

Quarantine Rule Set: Signatures of anomalous behavior used to detect and isolate a host on a network that is exhibiting suspicious activity until the behavior can be investigated.

Remediation – The act of correcting a vulnerability or eliminating a threat.

Removable devices: Hardware that an individual user can attach/connect to and detach/disconnect from a computer. Removable devices include: removable hard drives and CD/ROM readers.

Removable media: Physical object on which data is stored that an individual user can attach/connect to and detach/disconnect from a computer. Removable media includes: thumb drives, CDs, and DVDs.

[3] CNSS Instruction No. 4009, *A Common Information Assurance Glossary for National Security Systems*, (April 2010).
[4] CNSS Instruction No. 4009.